BIOMETRICS
DEPARTMENT OF DEFENSE

Presented by
Mr. Robert Kocher
Program Manager
DoD BMO/Ideal Innovations, Inc.

BIOMETRICS AND THE COMMON ACCESS CARD (CAC)

Phone: (703) 681-6446
Fax: (703) 681-6369
DSN: 761-6446

http://www.c3i.osd.mil/biometrics

Purpose

To provide an overview of DoD's Common Access Card (CAC) and strategy to demonstrate the viability of biometrics uses with or on the CAC.

❖

To provide an introduction to the CAC-Biometrics Working Group (CAC-BWG).

❖

Highlight issues of using biometrics with the CAC.

Positive Identification

Agenda

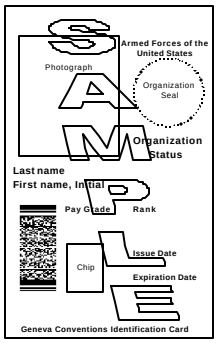
- **Overview of the Common Access Card (CAC)**
- **Rational for biometrics on or with the CAC**
- **Overview of the CAC-Biometrics Working Group (CAC-BWG):**
  - **Strategy**
  - **DoD Teams**
  - **Technology Demonstrators**

Positive Identification

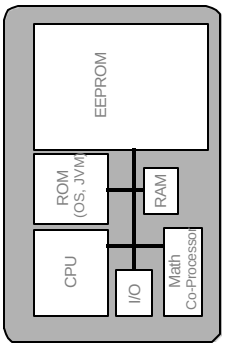
BIOMETRICS
DEPARTMENT OF DEFENSE

The Common Access Card (CAC)

Front



Inside



Back

Five Core Areas that make up the CAC

- Printed Data - Visually seen on front and back of card
- Code 39 Bar Code (on back) 1D bar Code
- PDF 417 Bar Code (on Front) 2D bar Code
- Mag Stripe (on Back) (On the smart card)
- Integrated Circuit Chip (ICC) (The smart card)

Positive Identification

BIOMETRICS
DEPARTMENT OF DEFENSE

Smart Card Decision

- **Dr. Hamre/Defense Management Council (DMC) decision on 24 Sep 1999 to adopt DoD Smart Card**
- **DEPSECDEF Memo, Subject: Smart Card Adoption and Implementation (dated 10 Nov 1999)**
- **DoD Common Access Card (CAC)**
  - **Provide physical and logical access**
  - **Military and civilian ID card**
  - **Platform for PKI hardware token (Class 3 maybe Class 4)**
- **Include multiple media (mag stripe, chip, bar code)**

Positive Identification

BIOMETRICS
DEPARTMENT OF DEFENSE

Who Receives a DoD CAC?

- **Active duty military**
- **Select Reservists**
- **DoD civilian employees**
- **Eligible DoD contractors**

(Approximately 4 million people)

Positive Identification

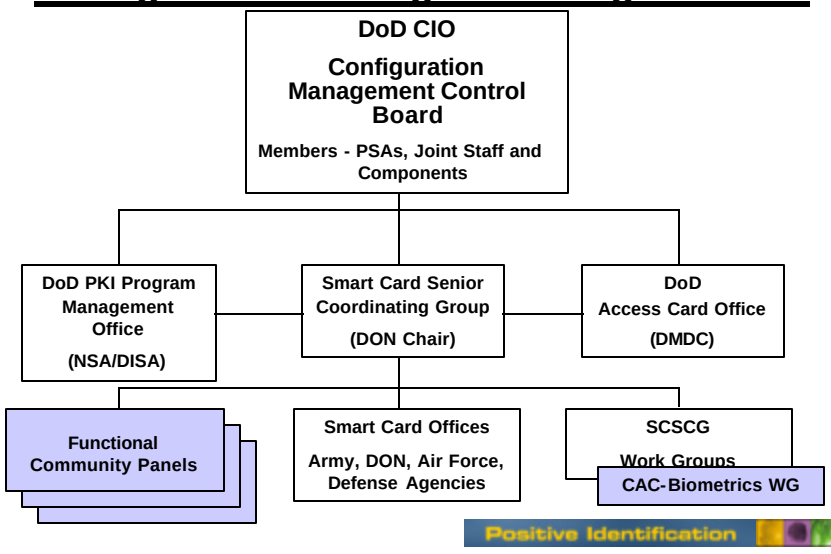
BIOMETRICS
DEPARTMENT OF DEFENSE

DoD CAC Vision

- **Commitment to innovation**
  - **Reform Business Processes**
  - **Exploit Technology**
  - **Achieve Efficiency**
- **Improved support of our warfighters**
- **Mission enhancement**
- **Readiness improvements**
- **Quality of life improvements**
- **Enhanced information assurance**

Positive Identification

Common Access/ID/Smart Cards Configuration Management Organization



Positive Identification

Rational for Biometrics on/with the CAC

- PIN Memory problems
  - ✓ Infrequent users
  - ✓ 6 to 8 digits
- 3 tries and card locks
- Unlocking revisiting issuance site
- Four million cards!
- Future applications
- Three factor authentication

Positive Identification

CAC-BWG Objectives:

(SCSCG Memorandum Aug 2001)

(1) "to coordinate and analyze requirements for the CAC-Biometrics,"

(2) "seek commonality in applications and interoperability"

(3) "assist CINCs, Services, Agencies and Functional Community Panels in the areas of biometrics use and integration with the CAC"

(4) "evaluate biometrics alternatives"

(5) "develop and recommend enterprise solution for biometrics with the CAC for approval of the SCSCG"

(6) "make recommendations to the SCSCG concerning CAC related
(6.a) biometrics hardware, software
(6.b) policy, and legal issues."

Positive Identification

CAC-BWG Teams:

- **Requirements - Survey Functional Community Panels and users to coordinate and analyze requirements.**
- **Technology - Identify and demonstrate technology alternatives and solutions for migration of the CAC to include Biometrics.**
- **Standards - Draft potential standards for integration of Biometrics with the CAC.**
- **Testing - Test and evaluate technology demonstrators. Coordinate demonstrators interactions with testing communities.**
- **Architecture – Develop and recommend the enterprise wide architecture.**
- **Kiosk – Near term approach to use biometrics to reset PIN or unlock CAC**
- **Policy – coordinate with Biometrics Policy Group on policy and legal issues.**

Positive Identification

Technical Demonstrations to an Enterprise Solution

Phase I-Part 1
Biometrics Demonstration
- **Focus on biometrics technology**
- **HW and SW**
- **Four Demonstration Scenarios**
- **Using the current CAC**

Phase II
System Demonstrations
- **Demonstrate Enterprise Solutions**
- **Security Testing**
- **Bio Applet Authenticate to Buffer**

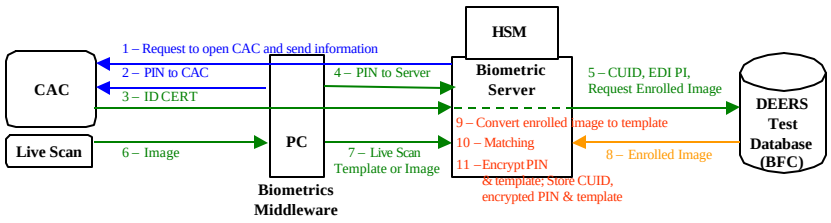
Phase 1-Part 2
Applet Modifications
- **Develop generic PIN/Key (Buffer) Solution**
- **Modifications PIN Management Process**

Positive Identification

Technical Demonstration Scenario 1

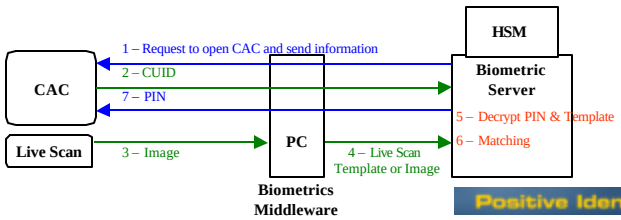
Template Store: Server
Biometric Match: Server

Scenario 1 – Biometrics Registration



Template Store: Server
Biometric Match: Server

Scenario 1 – Using Biometrics

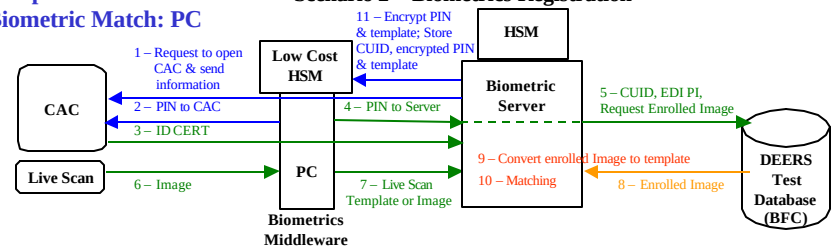


Positive Identification

Technical Demonstration Scenario 2

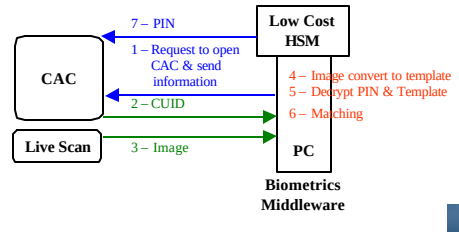
Template Store: PC
Biometric Match: PC

Scenario 2 – Biometrics Registration



Template Store: *PC*
Biometric Match: *PC*

Scenario 2 – Using Biometrics

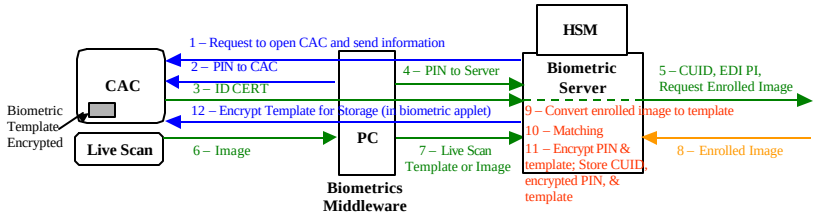


Positive Identification

Technical Demonstration Scenario 3

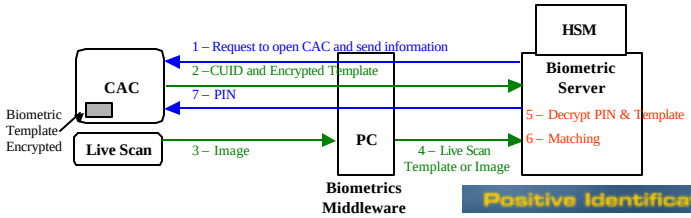
Template Store: Card
Biometric Match: Server

Scenario 3 – Biometrics Registration



Template Store: *Card*
Biometric Match: *Server*

Scenario 3 – Using Biometrics

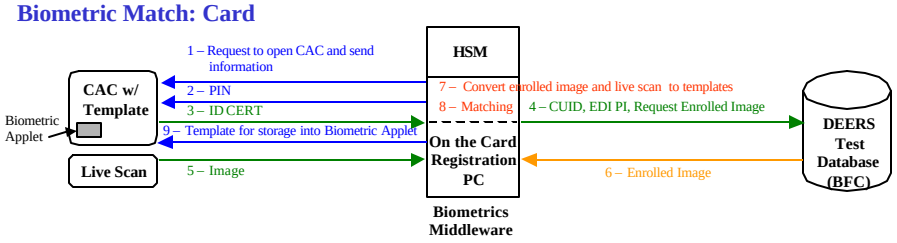


Positive Identification

Technical Demonstration Scenario 4

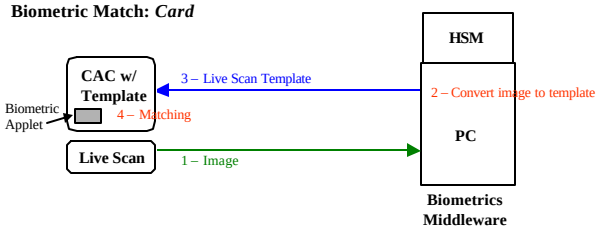
Template Store: Card
Biometric Match: Card

Scenario 4 – Biometrics Registration



Template Store: *Card*
Biometric Match: *Card*

Scenario 4 – Using Biometrics (PIN Internal Release)



Positive Identification

Conclusion

- **The CAC will enable DoD users with PKI.**
- **The CAC will be the access card to DoD information systems.**
- **Biometrics are currently an integral part of the CAC issuance process.**
- **There is support for implementing biometrics on or with the CAC. This will open a door to enterprise use of biometrics throughout DoD.**
- **Biometric systems for IA will have to be compatible with the CAC system.**

Positive Identification